**漏洞描述：**

上海甲鼎信息技术有限公司就业信息服务平台存在水平越权漏洞，攻击者可以通过修改PosiID 参数进行水平越权漏洞。

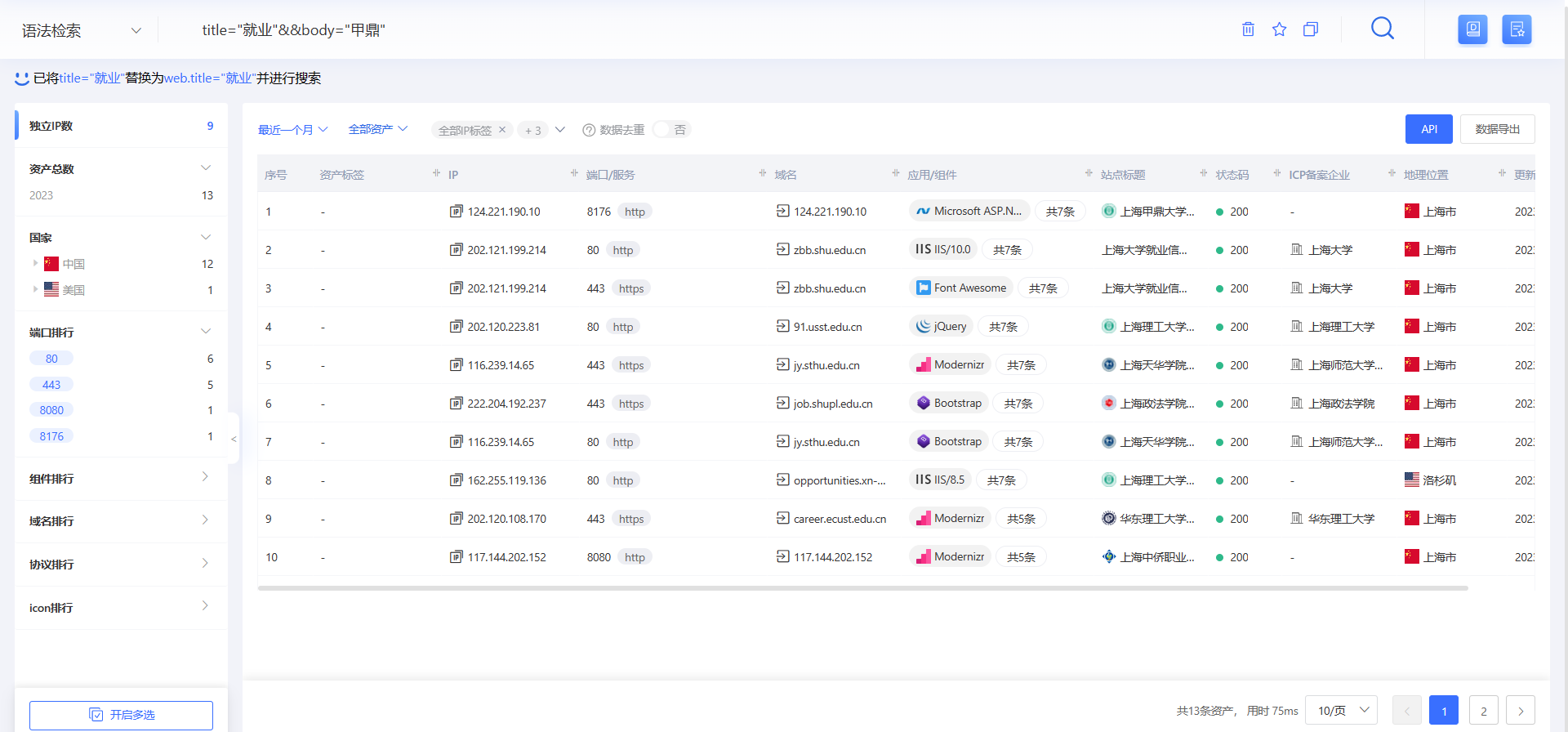
**公司主页：**

<http://www.infojiading.cn/gyjd.html>

**复现：**

鹰图语法：

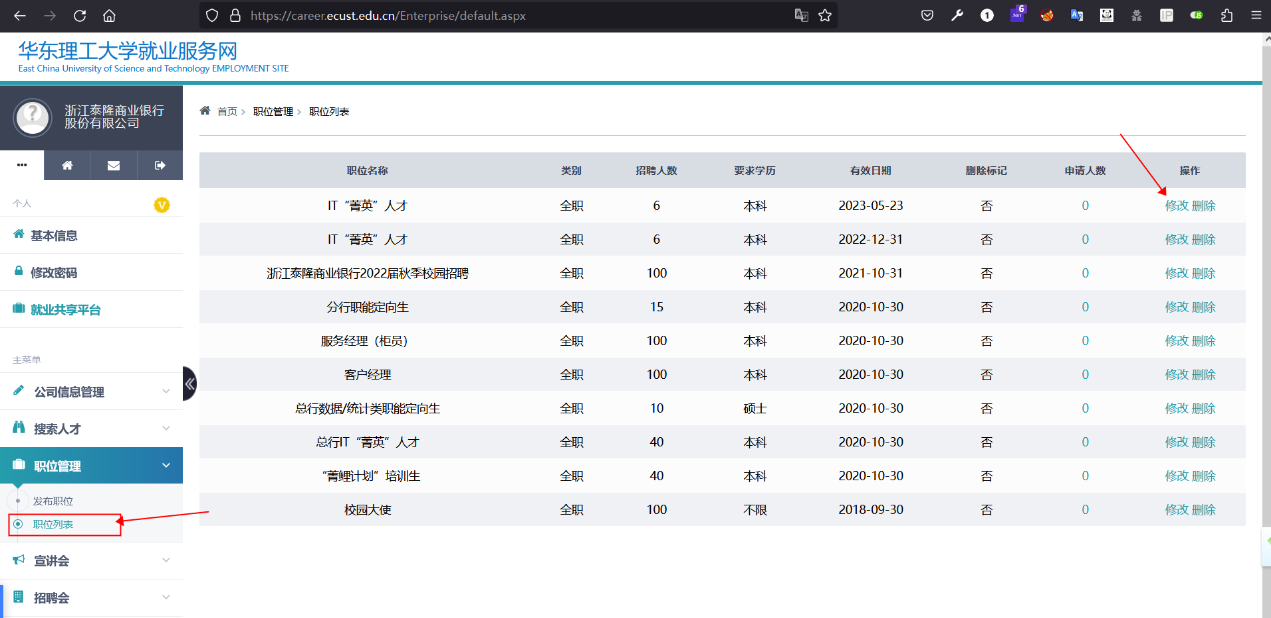
title="就业"&&body="甲鼎"



**案例一（华东理工大学）**：

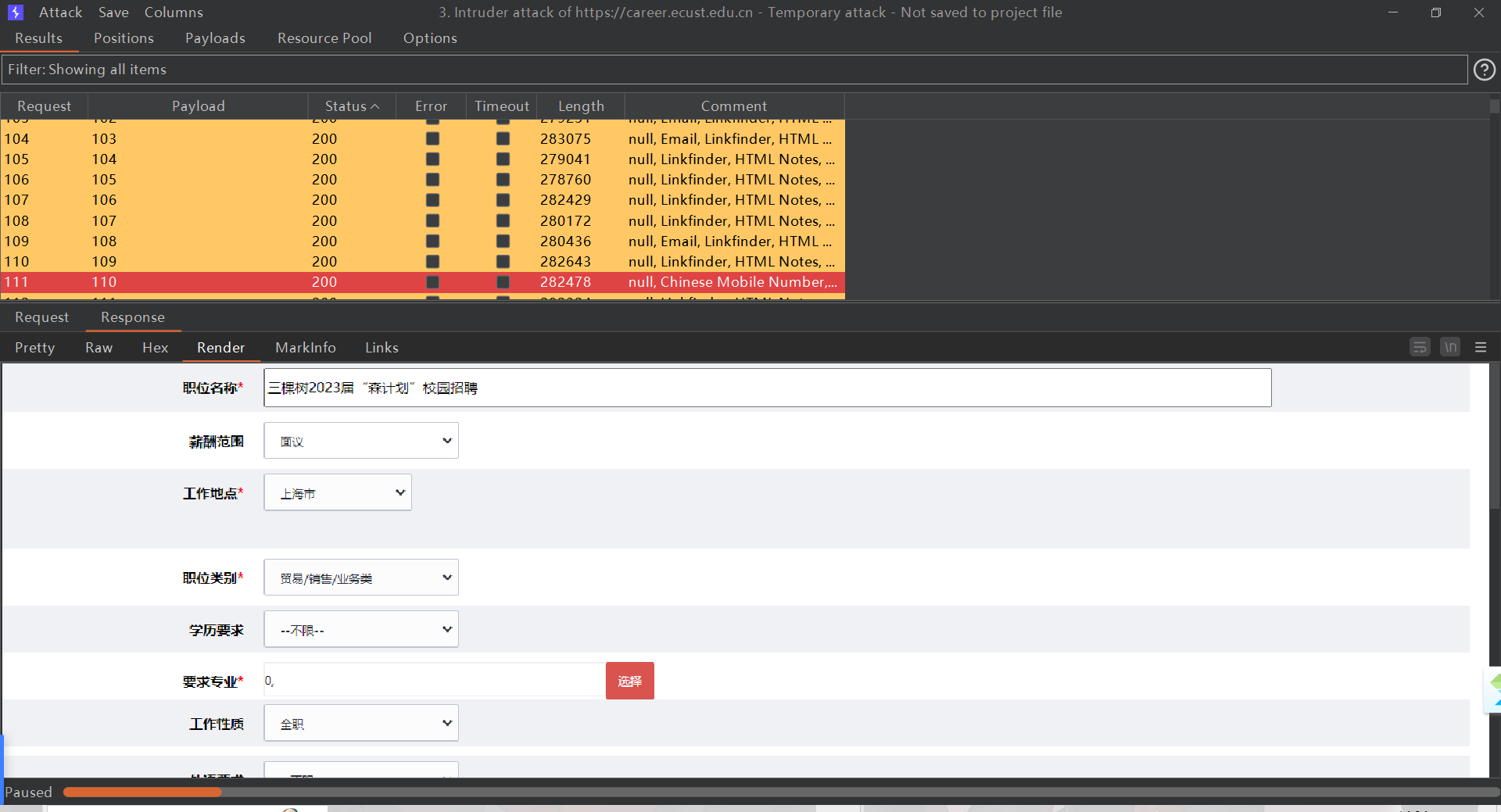
https://career.ecust.edu.cn/

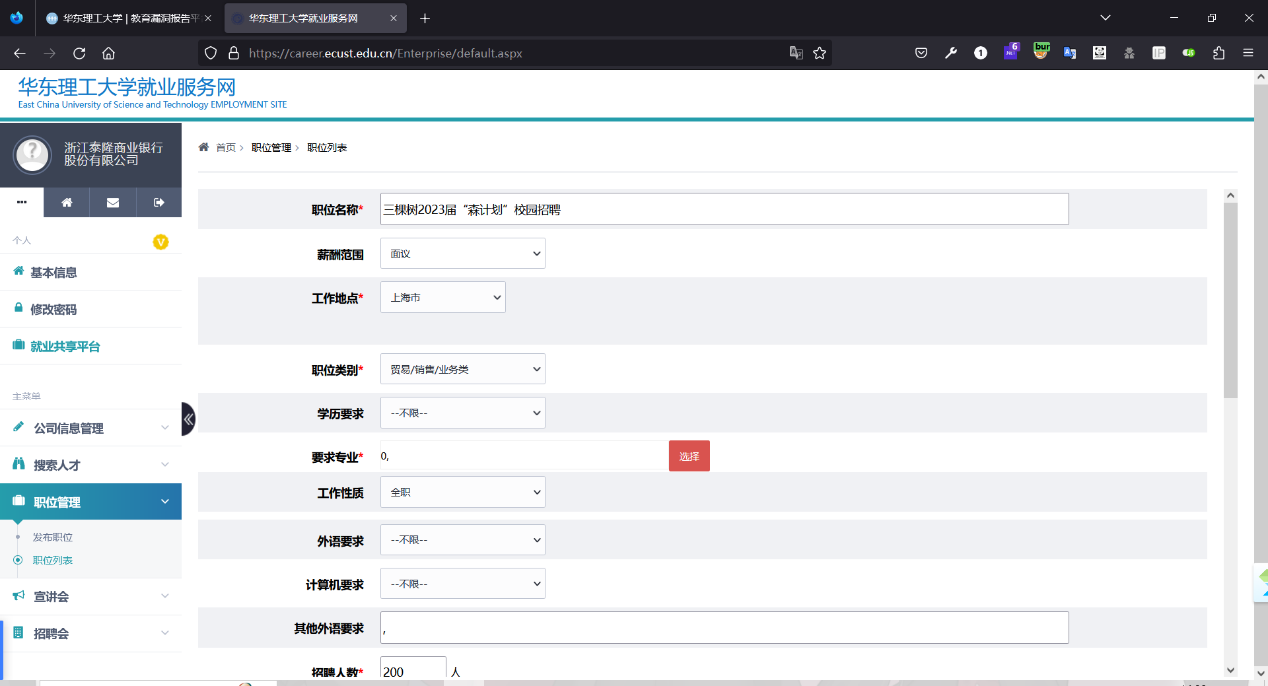
雇主账号密码：浙江泰隆商业银行股份有限公司、Admin123456



PosiID 参数存在越权，可任意修改其他公司职位列表



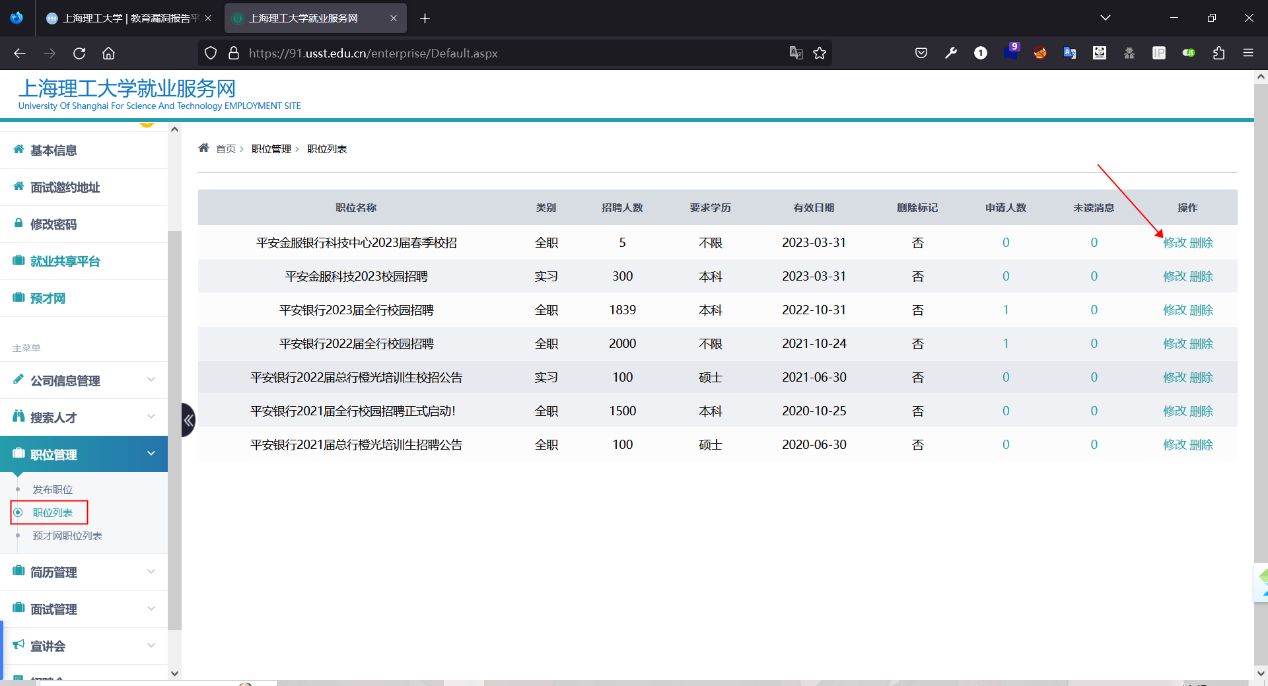




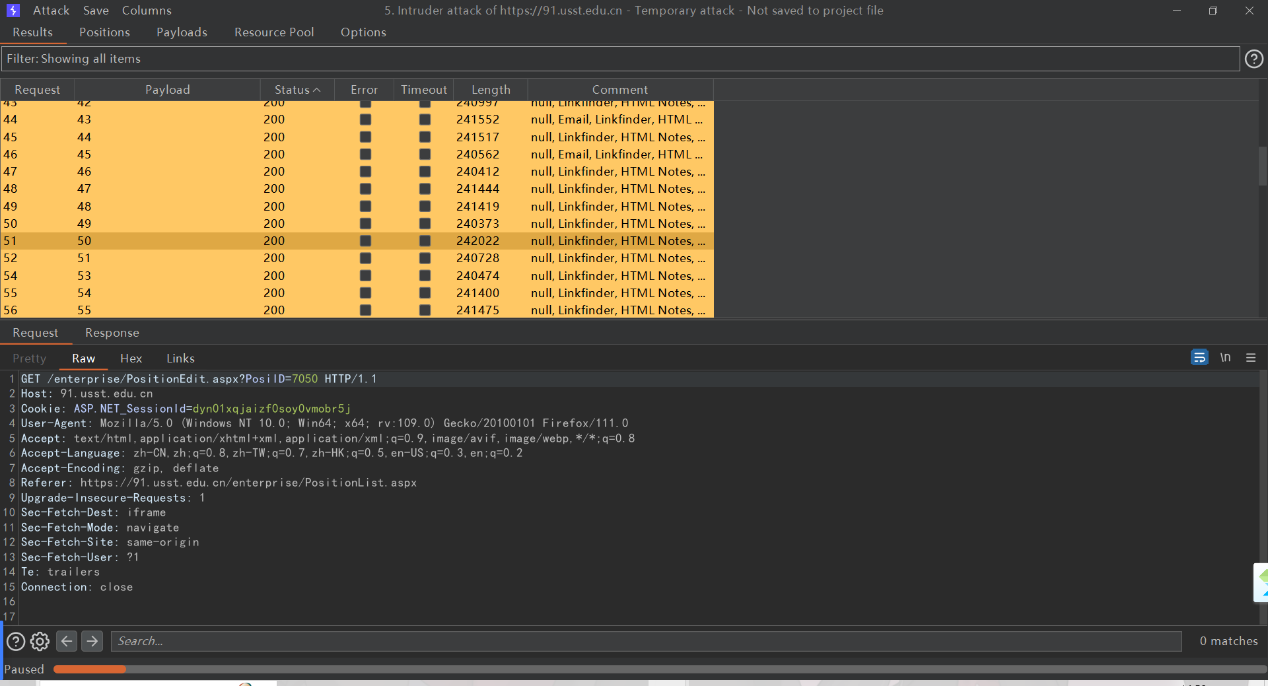
**案例二（上海理工大学）**：

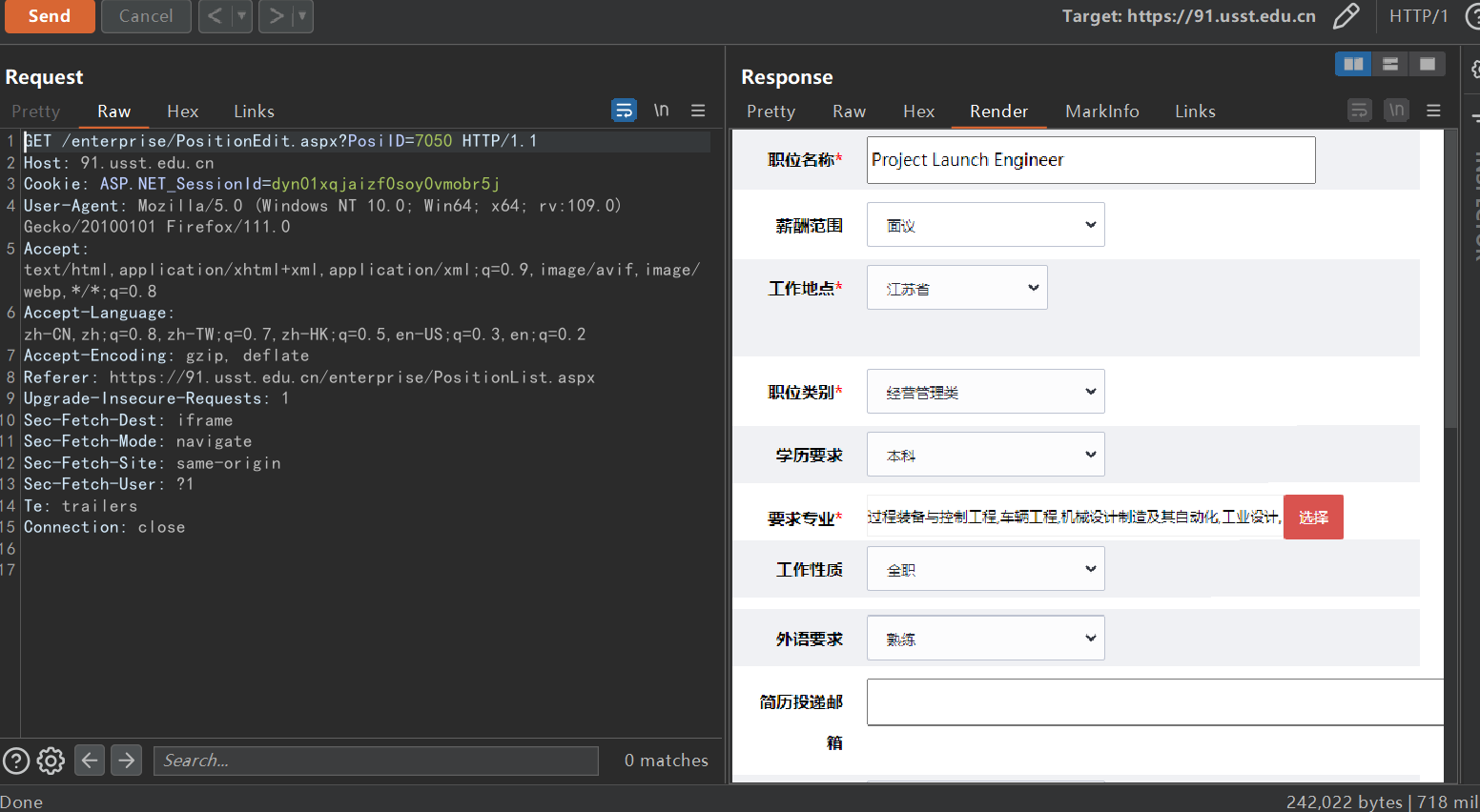
https://91.usst.edu.cn/

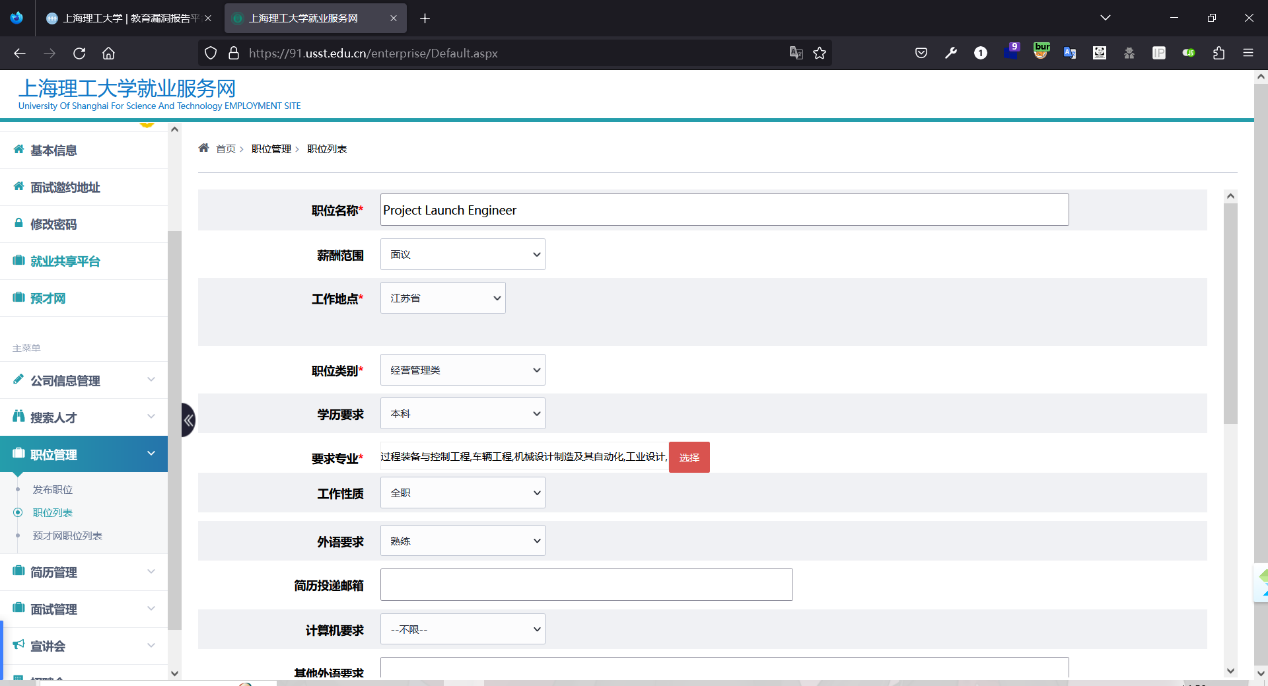
雇主账号密码：平安银行股份有限公司、Admin123456



PosiID 参数存在越权【这里只爆破了后两位】，可任意修改其他公司职位列表



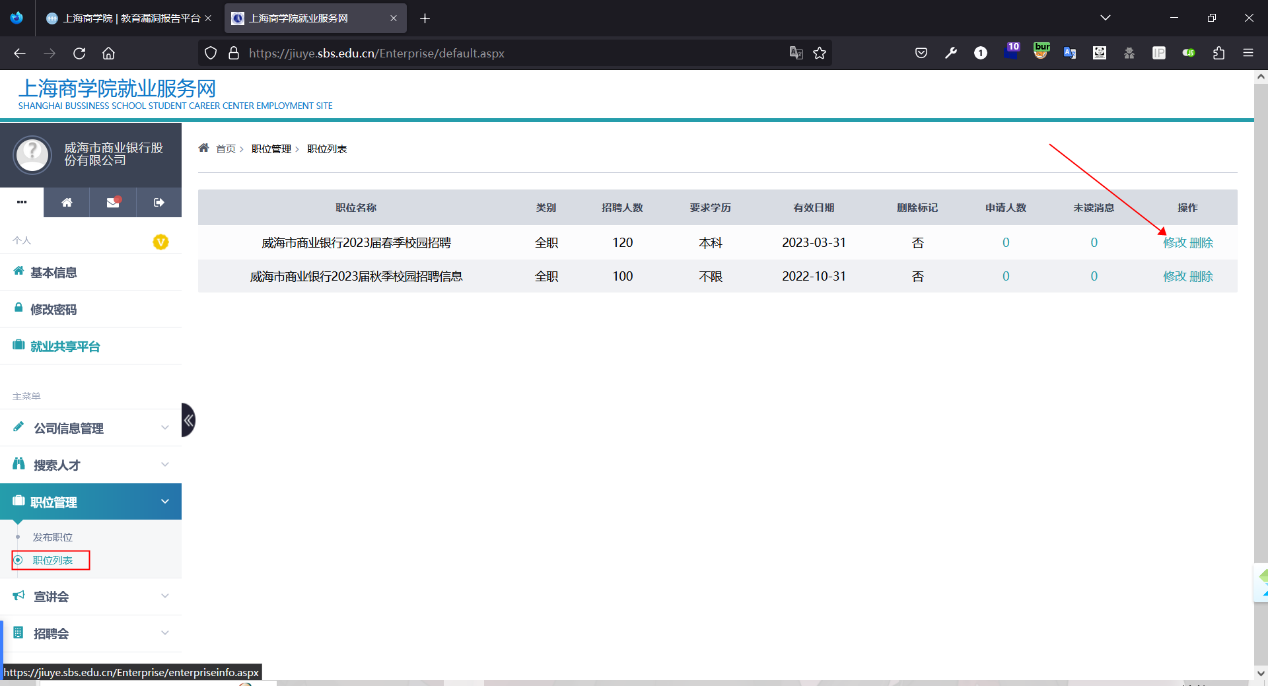




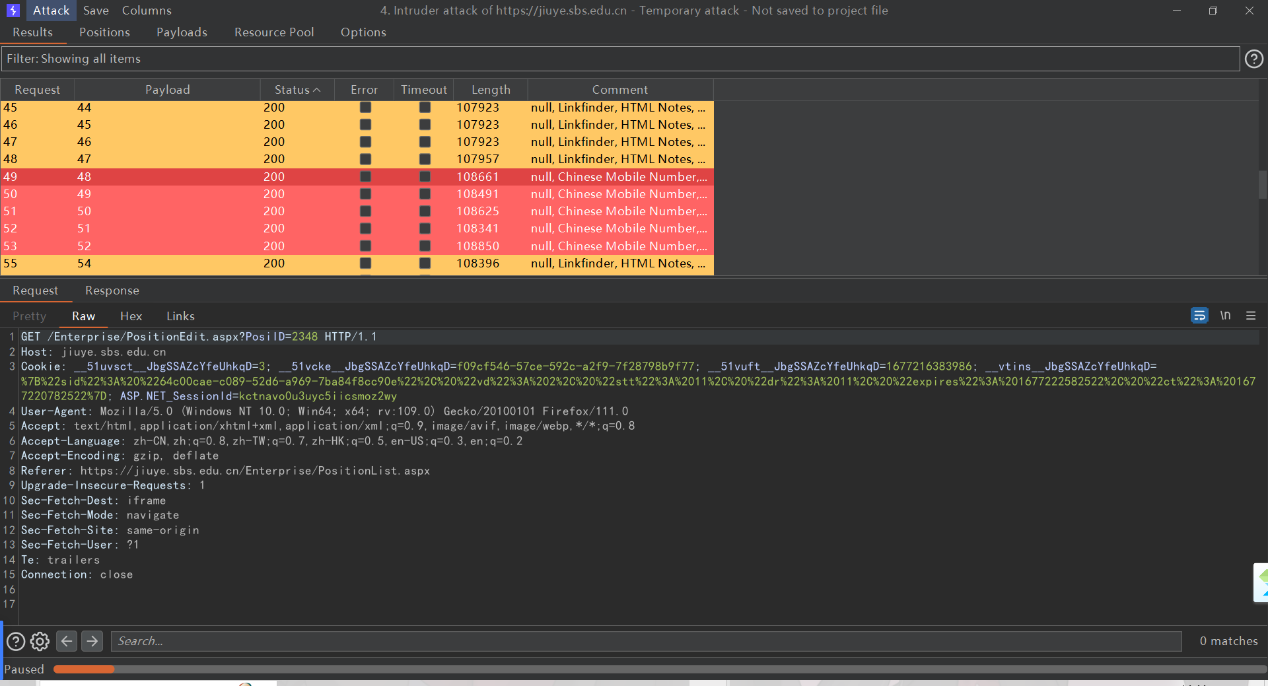
**案例三（上海商学院）**：

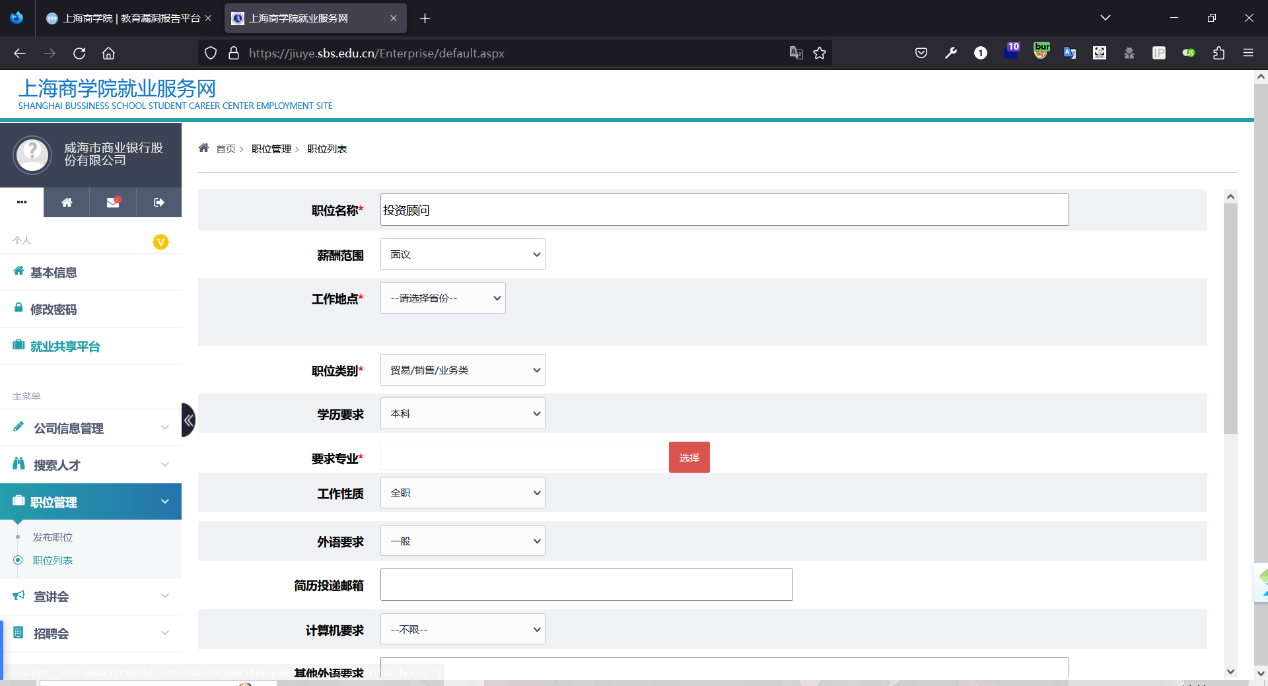
https://jiuye.sbs.edu.cn/

雇主账号密码：威海市商业银行股份有限公司、Admin123456



PosiID 参数存在越权【这里只爆破了后两位】，可任意修改其他公司职位列表





**其他地址：**

http://124.221.190.10:8176

http://zbb.shu.edu.cn

https://zbb.shu.edu.cn

http://91.usst.edu.cn

https://jy.sthu.edu.cn

https://job.shupl.edu.cn

http://jy.sthu.edu.cn

http://opportunities.xn--cesx9m.com

https://career.ecust.edu.cn

http://117.144.202.152:8080

https://job.shmtu.edu.cn

http://117.144.202.152

http://job.shmtu.edu.cn

**修复建议：**

1. 做好鉴权
2. 修改默认密码，提高密码强度